January 2021

Android Security

Nancy Mehra

ANDROID SECURITY

Nancy Mehra[1]
[1]Asst. Professor, Post Graduate Dept. of Computer Science, Arya College, Ludhiana, India

ABSTRACT

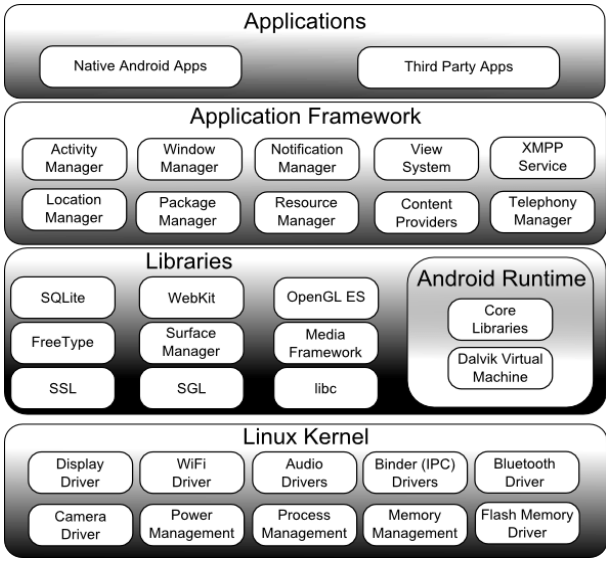
Android is the most popular mobile operating system among the most used touch devices. Today, 80 percentage of touch devices are using Android Operating System . The universality of Android devices has a direct impact on the app store Google Play, which was first introduced under the name of Android Market. Android is an open source operating system. Thus convincingly available and recognized by various operating system and code familiar to java , its applications can be easily developed and implemented on the Smartphones. Thousands of mobile apps are released through the Google Play Store every day ,so to measure the security here is difficult, as this number is increasing day by day. To guarantee the security of user's application, information, and data Android platform should be having a powerful security mechanism. The open source platform encourages the malicious software developers, to exploit and steal the user's private data.

Keywords: Android, Security , Smartphones

Introduction

With the increasing popularity of handheld and touch devices, there was an eager requirement of an operating system and it was fulfilled with the development of Android. The devices contain lots of features and functionalities that provide users with a way for an easy lifestyle. These features include hardware features such as audio, Bluetooth, camera, network, microphone, GSM, NFC, and sensors such as accelerometer, barometer, compass, gyroscope, and Wi-Fi. It also includes software features such as app widgets, home screen, input methods, live wallpapers, layouts, storage, messaging, multi-language support, browsers, Java support, media support, multi-touch, calls, messaging, multitasking, accessibility, external storage, and so on. Android offers millions of applications. It offers millions of applications on the Google play store and also they are increasing. In order to provide security for Open source platform, it requires a powerful and severe security architecture. With multi layered security, the architecture of Android platform is designed that gives the flexibility required for an open source platform. There are various security threats exists on Android phones, like Denial of Service attacks, colluding, repackaging apps to inject malicious code, permission escalation, and unauthorized access between the application. In this paper, various mobile security issues and recent android attacks will be discussed.

I Android Architecture



The Android Software Stack:

Android is architected in the form of a software stack comprising applications, an operating system, run-time environment, middleware, services and libraries. This architecture can, perhaps, best be represented visually as outlined in Figure above. Each layer of the stack, and the corresponding elements within each layer, are tightly integrated and carefully tuned to provide the optimal application development and execution environment for mobile devices[1].

Linux Kernel: It is the heart of android architecture that exists at the root of android architecture. The Linux Kernel is the bottom most layer in the Android architecture. The Android platform is built on top of the Linux 2.6 Kernel with a few architectural changes. The term kernel refers to the core of any operating system. The Linux Kernel provides support for memory management, security management, network stack, process management, and device management. The Linux Kernel contains a list of device drivers that facilitate the communication of an Android device with other peripheral devices. A device driver is software that provides a software interface to the hardware devices. In doing so, these hardware devices can be accessed by the operating system and other programs. The main reason of Linux kernel is because its open source. Anyone can go ahead and modify the Linux kernel without any hardware limitation or even any royalty issues.

Android Run Time:

Dalvik Virtual Machine: The Dalvik virtual machine was developed by Google . Dalvik VM is actually an interpreter for the Java programming language. The whole android runtime is written in Java in Android, and since all applications of android are written in Java it becomes much easier and smooth for the applications to run in the virtual environment[1].

Android Runtime – Core Libraries

The Android Core Libraries fall into three main categories:

Dalvik VM Specific Libraries: This is a set of libraries used for interacting directly with an instance of the Dalvik VM and is unlikely to be used by most Android application developer.

Java Interoperability Libraries: The Standard Java development environment includes a vast array of classes that are contained in the core Java runtime libraries. These libraries provide support for tasks such as string handling, networking and file manipulation (to name but a few) and are both familiar to, and widely used by Java developers regardless of platform.

Android Libraries[1].: This category encompasses those Java-based libraries that are specific to Android development. some key core Android libraries available to the Android developer is as follows:

- android.app – Provides access to the application model and is the cornerstone of all Android applications.
- android.content – Facilitates content access, publishing and messaging between applications and application components.
- android.database – Used to access data published by content providers and

includes SQLite database management classes.
- android.graphics – A low-level 2D graphics drawing API including colors, points, filters, rectangles and canvases.
- android.hardware – Presents an API providing access to hardware such as the accelerometer and light sensor.
    - android.util – A set of utility classes for performing tasks such as string and number conversion, XML handling and date and time manipulation.
    - android.view – The fundamental building blocks of application user interfaces.

Application Framework[1].

The Application Framework is a set of services that collectively form the environment in which Android applications run and are managed. This framework implements the concept that Android applications are constructed from reusable, interchangeable and replaceable components.

The Android framework includes the following key services:

- Activity Manager – Controls all aspects of the application lifecycle and activity stack.
- Content Providers – Allows applications to publish and share data with other applications.
- Resource Manager – Provides access to non-code embedded resources such as strings, color settings and user interface layouts.
- Notifications Manager – Allows applications to display alerts and notifications to the user.
- View System – An extensible set of views used to create application user interfaces.
- Package Manager – The system by which applications are able to find out information about other applications currently installed on the device.
- Telephony Manager – Provides information to the application about the telephony services available on the device such as status and subscriber information.
- Location Manager – Provides access to the location services allowing an application to receive updates about location changes.

Native Libraries[5]: Android includes a set of native libraries written in C/C++ which are compiled to native machine code. These libraries directly interact with Android Linux kernel and export its facilities to rest of the Android stack. On the top of linux kernel, their are Native libraries such as WebKit, OpenGL, FreeType, SQLite, Media, C runtime library (libc) etc.

- SQLite is a powerful and lightweight relational database engine. The same database engine is used in iPhone.
- Webkit is a fast HTML-rendering engine used by browsers. This is the same engine used in Safari, Chrome, Apple iPhone, and Nokia's S60 platform.
- OpenSSL is the secure socket layer for Internet security.
- Graphics libraries that include SGL and OpenGL for 2D and 3D graphics engines respectively. A surface manager provides a system-wide surface composer to render different drawing surfaces in a frame buffer. Instead of drawing directly to the screen, it makes use of the off-screen buffering. All the drawing commands go into off-screen bitmaps where they are combined with other bitmaps to form the final display the user will see. This allows Android to create visual effects like fancy transitions, transparent windows.

Applications[6]:

The applications are at the topmost layer of the Android stack. An average user of the Android device would mostly interact with this layer (for basic functions, such as making phone calls, accessing the Web browser etc.). The layers further down are accessed mostly by developers, programmers and the likes.

Several standard applications come installed with every device, such as:

- SMS client app
- Dialer
- Web browser
- Contact manager

II Mobile Security Issues[2]

1. **Data leakage**
   Data leakage is seen as being one of the most harmful threats to enterprise security. Android Operating system is widely used in the mobiles but still people are not aware about their OS and apps they are using. Many of apps which they are using may read their precious data without prior permission. Apps installed in mobile phones just need an access of storage and other permission to leak the data from device. So one should beware from installing unknown apps from unknown sources .

2. **Social Engineering**
   A staggering 91% of cybercrime starts with email, according to a 2018 report by security firm FireEye. The firm refers to such incidents as "malware-less attacks," since they rely on tactics like impersonation to trick people into clicking dangerous links or providing sensitive info. Phishing, specifically, grew by 65% over the course of 2017, the mobile users are at the greatest risk of falling for it because of the way many mobile email clients display only a sender's name — making it especially easy to spoof messages and trick a person into thinking an email is from someone they know or trust.

3. **Wi-Fi**
   A mobile device is secure if the network from it transmits data in secured. Today's era is public network era; we have to look after the public Wi-Fi before using this. It should be avoided unless we do not have second option. In an era where we're all constantly connecting to public Wi-Fi networks, that means our info often isn't as secure as we might assume.

4. **Out-of-date devices**

Smartphones, tablets and smaller connected devices — commonly known as the Internet of Things (IoT) —they generally don't come with guarantees of timely and ongoing software updates. This is true particularly on the Android front, where the vast majority of manufacturers are embarrassingly ineffective at keeping their products up to date — both with operating system (OS) updates and with the smaller monthly security patches between them — as well as with IoT devices, many of which aren't even designed to get updates in the first place.

5.**Password**

Password is something which assured the users that their data is safe. But is it true? How one be assured that one's application or data is secured by their passwords. Password comes in many forms like. Fingerprints , face locks, patterns, pins and etc. Which one from these is more secure? Fingerprints are secured because it cannot be same, face lock is secure but many cameras don't differentiate between people itself from their image. So choose the best password protections depending upon your device.

IV Recent Android Attacks[3]

Malware attacks on android mobile devices have increased very fast in past year. Hackers are attacking android smart phones with credential-theft, surveillance, and malicious advertising. Researchers examined that the cyber attacks in 2019 have risen by 50% compared with last year.

The key reason of increasing these attacks is use of mobile banking applications. Cybercriminals make them self more comfortable in attacking the mobile applications rather than internet banking (NEFT ETC).

In many cases, the malware attacks follow similar distribution strategies to those targeting desktop users, with the applications silently running in the background without the victim being any the wiser.

Some forms of Android malware have even been developed with advanced evasion techniques in order to remain undetected on infected devices.

For example, the Anubis banking trojan will only begin operating after motion sensors detect that the device has been moved -- a strategy to avoid it being detected and analyzed in sandbox environments.

V Identifying Android Malware[4]

The vast production and reduction in the cost with an increase in functionality and services are the reasons of the increasing demands of the smart phones especially android mobile phones.

Android malware can be characterized in different ways in a systematic characterization is proposed ranging from their installation, activation, to the carried malicious payloads. Malware installation can be generalized into three main social engineering-based techniques: repackaging, update attack, and drive-by download. Most of the malware package installed with the apps which are not installed from authorized sources. Some time while updating the application instead of enclosing the payload as a whole only an update component is included which will fetch or download the malicious payloads at runtime. Because the malicious payload is in the “updated” application, not the original application itself, it is stealthier than the malware installation technique that directly includes the entire malicious payload in the first place. The third technique applies the traditional drive-by download attack to mobile space.

VI Browser Security and Future Threat [7]

The increasing adoption of mobile devices and their use as a means to access information on the Web has led to the evolution of websites. Initially, mobile browsers had to access information through traditional websites. Today most of these websites also support Wireless Application Protocol (WAP) technology or have an equivalent mobile HTML.

In a typical Internet or WWW model, there is a client that makes a request to a server. The server processes the request and sends a response back to the client. This is more or less same in the WAP model, as well. However, there is a gateway or proxy that sits between the client and the server that adapts the requests and responses for mobile devices.

Mobile browsers are fully functional browsers with functionality that rivals desktop versions. They include support for cookies, scripts, flash, and so forth. This means that users of mobile devices are exposed to attacks

similar to those on desktop/laptop computers.

Conclusion

Mobile security must be ensured among all the Android devices. Even the authorized apps that are downloaded from the official app store are also at risk. Mobile app testing, device monitoring, forensics and security intelligence capabilities provide us with a unique set of mobile security data.

References

1. https://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture
2. https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html
3. https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/
4. https://www.intechopen.com/books/smartphones-from-an-applied-research-perspective/malware-analysis-and-detection-on-android-the-big-challenge
5. https://developer.android.com/guide/platform
6. https://androiddeveloperhelp.wordpress.com/2013/12/10/architecture-of-android-application/
7. https://books.google.co.in/
8. https://www.researchgate.net/